RESEARCH PLAN PROPOSAL

Impact of Security Issues and Analysis over Wireless Sensor Networks and their Integration with the Internet

For registration to the degree of
Doctor of Philosophy

IN THE FACULTY OF SCIENCE

THE IIS UNIVERSITY, JAIPUR

Submitted by

Ayush Sogani
Enroll. No.: IISU/2010/177

Under the Supervision of

Dr. Aman Jain
Professor & HOD (CS)
Deepshikha College of Technical Education, Jaipur

Department of Computer Science

July & 2012

1. **Topic**

Impact of Security Issues and Analysis over Wireless Sensor Networks and their Integration with the Internet

2. **Introduction**

Wireless Networks:

Wireless network refers to a computer network that is not connected by cables of any kind. It is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations.

Sensor Networks:

A sensor network is a group of specialized transducers (A transducer is an electronic device that converts energy from one form to another. E.g., Antenna) with a communications infrastructure intended to monitor and record conditions at diverse locations. A sensor network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable.

Wireless Sensor Networks: (Wireless Communication+ MEMS)

Wireless communication and MEMS (Micro-Electro-Mechanical Systems), the two technologies modernized together as the way we want and have resulted in the development of Wireless Sensor Networks. Wireless sensor networks are composed of large numbers (up to thousands) of tiny radio equipped sensors. Every sensor node has a small microprocessor with enough power to allow the sensors to autonomously form networks through which sensor information is gathered. Sensor nodes in such networks are ad hoc deployed, self-configurable and battery powered.

3. **Review of Literature**

3.1 Introduction

Wireless Sensor Networks are currently receiving significant attention due to infinite possibilities available with them. Researchers have focused on different research challenges that have limited capabilities i.e., security, deployment over Internet,

power, and localization.

Most research is currently being conducted in the following areas:

- Developing techniques that will enforce secure, private and reliable networks.
- Deployment and Integration of WSN with Internet & recent technologies and impact of different security issues.
- Improving reliability of data transfer (connecting WSN with TCP/IP networks).
- Increasing network lifetime (Energy Consumption).

Cheap, smart devices with multiple onboard sensors, networked through wireless links and the Internet & deployed in large numbers, provide extraordinary opportunities for instrumenting and controlling homes, cities, and the environment, this is a technology of future, the Networked microsensors technology[1].

These sensors are becoming smaller. It is possible to fit them into a smaller volume with more power and with less-production costs. This becomes possible with the help of Microelectromechanical Systems (MEMS) technology [2].

Wireless sensor networks (WSN) are abbreviated wireless networks of small, low-cost sensor nodes, which collect and distribute environmental data. WSNs helps in monitoring and controlling of physical environments from remote locations with better accuracy than other known monitoring systems such as remote sensing. These tiny sensor nodes leverage the idea of sensor networks based on collective effort of a large number of nodes. Sensor networks represent a significant improvement over traditional sensors. As they have the capabilities to route data back by a multi- hop infrastructureless architecture to the base station or sink, which is the entity where information is required. The sensor nodes unite together to collect desired information from the environment by performing in-network data processing and aggregation (data diffusion).

A sensor device consists of the following components:

- **Sensing Unit**: It helps to sense and measure physical data from the target area.
- **Processing Unit**: The processing unit plays a major role in managing

collaboration with other Sensors to achieve the predefined tasks. The processing unit needs storage for tasking and to minimize the size of transmitted messages by local processing and data aggregation [3].

- **Transceiver**: Three communication schemes for deployment in sensors are optical communication (laser), infrared and radio-frequency (RF). Laser consumes less energy than radio and provides high security, but requires line-of-sight and is sensitive to atmospheric conditions. Infrared needs no antenna but is limited in its broadcasting capacity. RF is the most easy to use and requires antennas.
- **Power Unit**: Batteries used in sensors can be categorized into two groups; rechargeable and non-rechargeable. In unapproachable conditions, it is impossible to recharge or change a battery. Therefore, power management is a critical research issue in Wireless Sensor Networks [4]. Two major power saving approaches has been defined. First, unused devices can be shut down and activated when required. This is called Dynamic Power Management (DPM) and second approach is Dynamic Voltage Scheduling (DVS), power can be varied to allow for a non-deterministic workload [5].

The figure of sensor device components is shown in Appendix Fig 1.

Many wireless sensor network applications cannot run in complete isolation; the sensor network must be connected to monitoring and controlling entities through known wireless/wired networks like IP-based networks. Such interconnection achieves many advantages and increases sensor networks benefits such as:

- Controlling and monitoring sensor networks remotely.
- Providing security at the gateway node
- Integrating data collected from sensor networks into data mines.
- Ability to combine multiple remote sensor networks into one virtual sensor network.

3.2 Sensor Network History

The development of sensor networks requires technologies from three different research areas: sensing, communication, and computing (including hardware,

software, and algorithms). Thus, combined and separate advancements in each of these areas have driven research in sensor networks.

Since the early 1950s, a system of long-range acoustic sensors (hydrophones), called the Sound Surveillance System (SOSUS), has been deployed in the deep basins of the Atlantic and Pacific oceans for submarine surveillance. Beams from multiple hydrophone arrays are used to detect and locate underwater threats. Recently, SOSUS has been replaced by the more sophisticated Integrated Undersea Surveillance System [1].

3.3 Implementation of Transport Layer Protocol

Wireless sensor networks require several attributes such as fault tolerance and scalability. The relatively short lifetime of a sensor is an additional factor when deploying sensors in a target area. Message loss may be a serious problem. Developing a reliable transport protocol for wireless sensor networks to support more applications deployment is an important issue so that the loss of data can be prevent. TCP to wireless sensor networks is expensive because of its three-way handshake mechanisms and packet header size. UDP is considered to be more suitable for sensors although it was designed to provide unreliable data transport [2]. Few new mechanisms are intended to enable the use of TCP/IP for wireless sensor networks: spatial IP address assignment, header compression, application overlay routing and distributed TCP caching (DTC) [7].

3.4 Integration Future Large-scale Wireless Sensor Networks with the Internet

For practical deployment, a sensor network does not work in isolation. For many important applications, however, it is required to integrate these sensor networks to the existing Internet Protocol (IP) networks.

The task of connecting WSN to the existing Internet brings with it several challenges [9]. Any network wishing to be connected to the Internet needs to address the question of how it will interface with the standard protocols like the IP. The characteristics of WSN make them different from traditional IP-based networks as summarized in Annexure Table 1. The chief among these are that WSN are large-scale unattended systems consisting of resource-constrained nodes that are best-suited to application-specific, data-centric routing.

Giving IP address to every sensor node is not the right approach to integrating sensor networks with the Internet. For this purpose a gateway level protocol approach is developed for both homogeneous networks (where all nodes have the same capability in terms of processing, energy and communication resources) and heterogeneous networks (where some nodes are more capable compare to other nodes). Application level gateway solution is used in integration of Homogeneous networks and the Internet and an overlay IP network (router) is constructed in case of Heterogeneous networks that sits on top of the basic wireless sensor network.

3.5 Security Issues in Wireless Sensor Networks

Sensor networks position unique security challenges because of their inherent limitations in communication and computing. The deployment nature of sensor networks makes them more vulnerable to various attacks. Sensor networks are deployed in applications where they have physical interactions with the environment, people and other objects making them more vulnerable to security threats.

Security goals in sensor networks depend on the requirements of the user to know what users want to protect. Four goals are determined in sensor networks. They are Confidentiality, Integrity, Authentication and Availability [10].

- **Confidentiality** is the ability to hide message from a passive attacker, where the message communicated on sensor networks remain confidential.
- **Integrity** refers to the ability to confirm the message has not been altered, or changed while it was on the network.
- **Authentication** Need to know if the messages are from the node it claims to be from, determining the consistency of message's origin.
- **Availability** is to determine if a node has the ability to use the resources and the network is available for the messages to move on.

Few attacks [10] are also identified in wireless sensor networks, they are:

- Passive Information Gathering
- Node Malfunctioning
- Message Corruption
- Traffic Analysis
- Wormholes
- Hello flood Attacks

- Denial of service Attacks.

3.6 Integrating Wireless Sensor Networks and the Internet: A Security Analysis

Access to the information produced by sensor networks has not been considered intensely. Once the data is retrieved from the sensors, the user of the network will be able to read it directly through the base station. This access to the data must be challenged and a security mechanism must be defined for the user authentication. This can be achieved by integrating the sensor networks into the Internet. Sensor networks must be secure by themselves, and the interactions between the sensor networks and the Internet must also fulfill with certain security properties [8]. The integration strategies are shown in the Appendix Fig 2.

In front-end proxy solution, the base station serves as an interface between the data acquisition network (sensor network) and the data dissemination network (the Internet). The base station collects and stores all the information coming from the sensor network, and also sends any control information to the sensor nodes. There is no direct connection between the Internet and a sensor node: all incoming and outgoing information will be parsed by the base station [8].

In the gateway solution, the base station acts as an application layer gateway, in care of translating the lower layer protocols from both networks (e.g. TCP/IP and proprietary). As a result, the sensor nodes and the Internet hosts can exchange information directly.

In the TCP/IP overlay solution, sensor nodes do communicate with other nodes using TCP/IP. Therefore, the main function of the base station is to perform as a router, forwarding the packets from and to the sensor nodes. These nodes must implement the protocols and standards used on the Internet, such as the TCP/IP stacks and web services interfaces [8].

Sensor networks are not integrally secure. Its nodes must be deployed near the source of the events, and they use wireless communication channels for exchanging data. Therefore, any nasty challenger can manipulate the sensor nodes, the environment, or the communication channel on its own benefit. Besides, if that malicious outsider gains access to one or more sensor nodes, it may be possible to deploy the information flow that navigates the nodes. Therefore, a sensor network must be

designed from hardware of its nodes to their application layer to protect or reduce the effect of such attacks.

3.7 Encryption and Key Management Approach with In-Network Processing in Wireless Sensor Network and Security Analysis

A sensor network is a combination of three different nodes: normal sensor nodes, aggregators, and a querier. Aggregator collects the information from the normal sensor nodes available in the sub-network with the help of a suitable aggregation function and then transmits the result to the higher aggregator or to the querier (query generator). A communication gets established between these nodes and a meaningful information is derived which reflects the events in the target field. The major problem faced by wireless sensor network is through the transmission of data from one intermediate node to another node. Hence security becomes a very important issue, as the information transmit between the nodes in a hierarchical sensor environment, only the authorized sensors should have the cryptographic keys by which they can decrypt the encrypted information. Thus a requirement of different access control policies occurred at each level of the hierarchical network. Sensor networks require protection against eavesdropping, injection and modification of information like traditional networks does. Therefore the requirement is of such a network where the message should be transferred in a confidential way. Opponents that eavesdrop communication between the sensors, aggregators, and the sink shall not obtain the exchanged information. This is achieved by encrypting transmitted data. Therefore, Cryptography becomes the standard defense mechanism. If the encryption key is not distributed properly with a proper research then this key will be available for all the nodes and intruder can easily retrieve it and take the information from the cipher text. Therefore, key management and aggregation are the important problems in wireless sensor networks on which lot of research is still required.

End to end encryption for wireless sensor networks is a challenging problem. The communication inside the network consumes a large amount of the total energy of the WSN. To save the complete energy resources of the network it is approved that sensed data need to be shared and aggregated. If end to end encryption is preferred, then distributing usual encryption algorithms implies that intermediate nodes have no possibility for efficient aggregation allowing shrinking the size of messages to be

forwarded. This approach of usual encryption algorithms combined with the necessity of efficient data aggregation provides only the possibility of encrypting the messages hop-by-hop. This means that an aggregator has to decrypt each received message, then aggregate the message according to the matching aggregation function and, finally, encrypt the aggregation result before forwarding it[11].

For point-to-point communication, end to end cryptography attains a high level of security but requires that keys must be set up among all the end points and be unsuited with passive participation and local broadcast. Link -layer cryptography with a network-wide shared key simplifies key setup and supports passive participation and local broadcast, but in this case the intermediate nodes might eavesdrop or alter messages. Therefore, an evaluation of the network traffic is carried out to calculate the measure of the attacker's ability to compromise a message traversing a particular route. An intelligent attacker can easily guess the vulnerability of traffic and initiate attack on the nodes by observing the network topology and gathering information from the hidden data aggregation and homomorphic encryption. There is a resource expenditure associated with the attacking of nodes and extraction of keys from the memory. Hence, the best attack strategy is the one in which a set of nodes are attacked with minimum total resource expenditure. Thus through this proposal it can be seen that aggregated consideration of information from the concealed data aggregation and privacy homomorphism protocols can lead to a major reduction in resource expenditure[12].

3.8 Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN)

In today's scenario, when technologies are growing very fast and frequently, people are adopting these new concepts like wireless sensor networks (WSN), cloud computing, pervasive computing, etc., in their daily life. Wireless Sensor Networks (WSN) are becoming popular day by day, but there are some issues in wireless sensor networks such as energy consumption, processing time, memory usage, resource limitation and security. Keeping in mind about all these issues, different cryptographic techniques such as symmetric key and asymmetric key cryptography are investigated.

Cryptographic algorithm plays an important role in the security protection of wireless sensor networks (WSN). Different encryption techniques like stream cipher (RC4), block cipher (RC2, RC5, RC6, etc.) and hashing techniques (MD2, MD4, MD5, SHA, SHA1, etc.) are compared with each other by selecting different comparison problems.

After performing simulation of these algorithms it was found that public key is not energy efficient and is expensive in terms of both computation and communication as compared to symmetric key. As sensor networks have limited resources, therefore most of the researcher used symmetric keys in WSNs. Thus it was concluded that symmetric key techniques are more feasible for WSNs as compared to public key. More comparisons are applied on different encryption techniques and it was concluded that RC5 is feasible and consumes less energy/resources as compared to other algorithms (AES, MD5, and SHA1). Finally, it was proposed that RC5 is a best algorithm to create Message Authentication Code (MAC) in sensor networks [13].

4. Motivation to the Work

Current research in the areas of wireless communications, micro-electromechanical systems and low power design is progressively leading to the development of cost effective, energy efficient, multifunctional sensor nodes. Sensing, communication, processing and battery units are the primary components of a sensor node. Individual sensors have the capacity to detect events occurring in their area of deployment. Reliable and secure data transport is an important feature of dependability and quality of service in several applications of wireless sensor networks. Routing protocols providing an optimal data transmission route from sensor nodes to sink (active node) to save energy of nodes in the network. Data aggregation plays an important role in energy conservation of sensor network. Data aggregation methods are used not only for finding an optimal path from source to destination but also to eliminate the redundancy of data, since transmitting huge volume of raw data is an energy intensive operation, and thus minimizing the number of data transmission. Also multiple sensors may sense the same phenomenon, although from different view and if this data can be reconciled into a more meaningful form as it passes through the network, it becomes more useful to an application. These sensor nodes

have a critical piece of information that is to be sent to the sink (active node). To manage and hold the information by the sensor nodes for a long period of time is not possible due to the lack of energy, computation and communication capabilities and it is also unsecured to put data in sensor node for a long period of time because of their inherent limitations. Therefore, there must be a secured platform available that can take the information from the sensor nodes and store them securely. Now days Internet is the best platform where we can save the information generated from the sensor nodes. Due to inherent limitations in sensor networks security is an area where lots of research work is to be taken place and the complete integration of sensor networks and the Internet is still under research work. During this integration process security is always been a challenging issue. Therefore a schema is required which gives a completely integrated secured Internet based sensor network. These limitations and the requirement of such a schema, gives motivation towards development of an Internet based secure sensor network.

5. Objectives

Recent advances in wireless communication and embedded computing technologies have led to the rise of wireless sensor networks technology. These nodes can be deployed in many fields including health, environment and battlefield monitoring and represent a big source of varied data. In order to support huge amounts of data, today solutions are based on different Internet Applications. Accordingly, it seems obvious to bring wireless sensor networks to the Internet. However, this integration process raises many key challenges. Among them security, localization and power management are few problems and may be the most critical is the security of sensor networks, the interaction between these networks and the Internet.

1. The goal of this research is to study how possible is the integration of wireless sensor networks with Internet and to assess its impact on different security issues and analysis.
2. A schema would be defined for the Internet based wireless sensor networks and propose optimization solutions based on data aggregation and several security mechanisms to maximize the security and privacy issues.

3. An Algorithm will be proposed which will define the best security mechanism and method, which can be implemented in between the integration of wireless sensor networks with Internet.
4. This research also proposed a security framework to provide countermeasures against attacks in wireless sensor networks using different cryptographic techniques like symmetric key and asymmetric key encryptions techniques.
5. This research will be consistent with the next generation Network (NGN) to support pervasive computing (Anytime Anywhere).

6. Plan of Work and Methodology:

Work Plan (Including Gantt chart):

For the first 6-7 Months: *In depth study on existing applications for integrating wireless sensor networks with the Internet.*

Description: At the end of this step, we will have a good knowledge of Internet based applications, wireless sensor networks and the existing solutions for their integration and also know about the key challenges of this issue.

Document: Description of existing agendas while pointing out for each one the benefits and the drawbacks.

At least 10-12 months are required for: *Proposing a schema for Internet based wireless sensor networks.*

Description: During this step, we will focus on the real integration of wireless sensor networks with Internet using simulation tools or/and real platform. At the end of this step, we would be able to show a demonstration of the work done.

Document: Mainly a description of the proposed schema as well as difficulties and solutions to realize the integration.

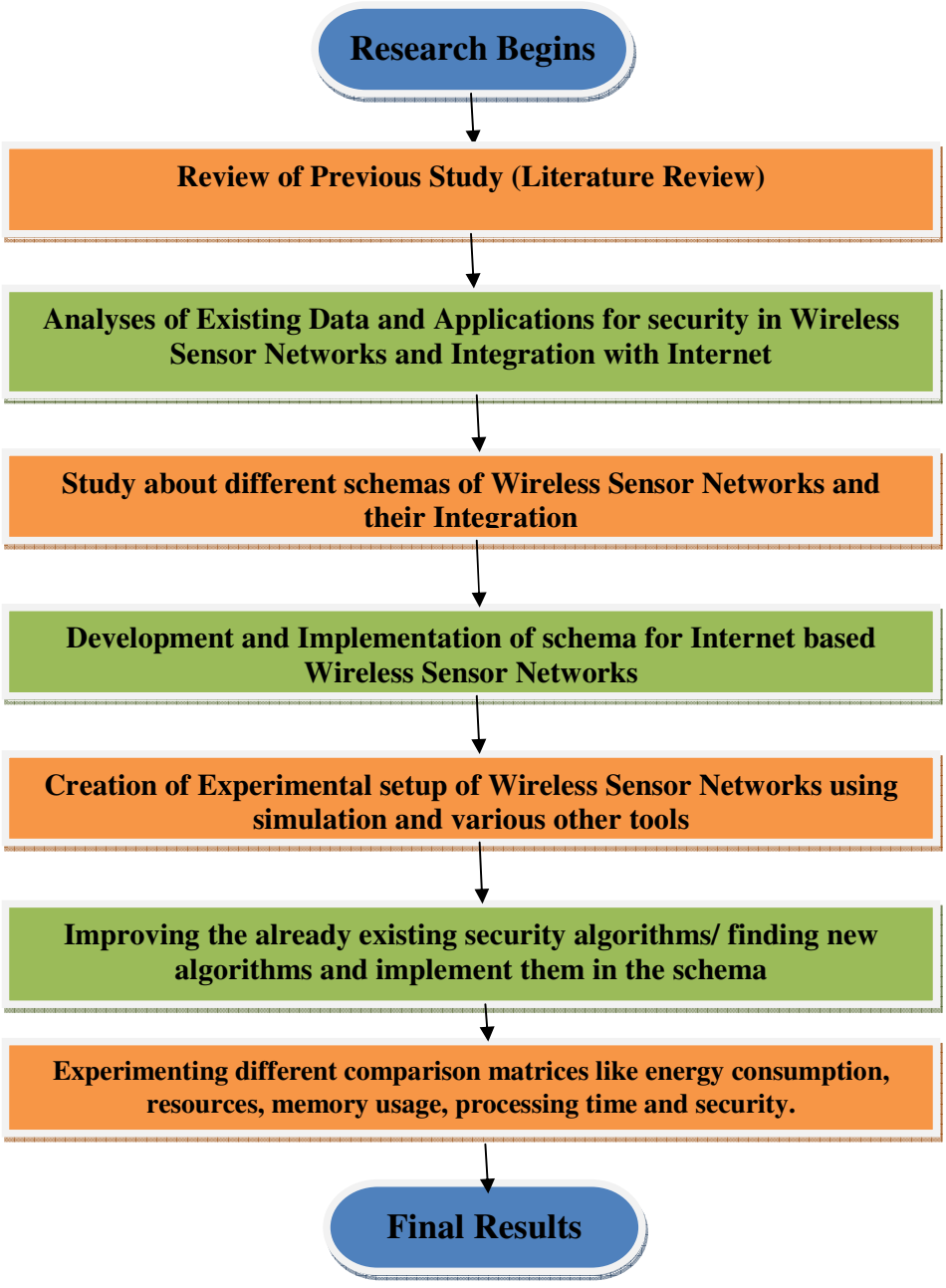
7-8 months for: *Data aggregation and Security mechanisms will be optimized and implementation of secured network schema in Internet will be defined.*

Description: Based on the previous schemas, we will focus on data aggregation and security mechanisms in order to make best use of security issues. Then, we will evaluate the performance of the given proposals.

Document: Description of the proposed approach for security level and comparison with existing solutions.

Methodology & Tools to be used:

Methodology


Research Begins
Review of Previous Study (Literature Review)
Analyses of Existing Data and Applications for security in Wireless Sensor Networks and Integration with Internet
Study about different schemas of Wireless Sensor Networks and their Integration
Development and Implementation of schema for Internet based Wireless Sensor Networks
Creation of Experimental setup of Wireless Sensor Networks using simulation and various other tools
Improving the already existing security algorithms/ finding new algorithms and implement them in the schema
Experimenting different comparison matrices like energy consumption, resources, memory usage, processing time and security.
Final Results

- Different approaches can be considered to connect a Wireless Sensor Network with the Internet and analyses the security of their interaction.
- For this purpose, these are the following **tools** that can be used:

TinyOS – A Linux based simulation tool which is used to design and configure the Wireless Sensor Networks. Different security mechanisms can also be configured using this tool.

OMNeT++4.x - is a component-based discrete event simulator. OMNeT++ uses building blocks called modules to implement their simulation. Modules are connected in a hierarchical nested fashion, where each module can contain several other modules. Regarding simulation of WSN and IP networks, OMNeT++ relies on external extensions. The two most prominent ones are the INET Framework for IP network and Castalia for WSN. The OMNeT++ 4.x Integrated Development Environment is based on the Eclipse platform, and extends it with new editors, views, wizards, and additional functionality. OMNeT++ adds functionality for creating and configuring models (NED and ini files), performing batch executions, and analyzing simulation results, while Eclipse provides C++ editing, SVN/GIT integration, and other optional features (UML modeling, bugtracker integration, database access, etc.) via various open-source and commercial plug-ins.

WiSeNet Simulator is a free and open-source utility that is designed to develop a platform for the evaluation of secure routing protocols in Wireless Sensor Networks.

Other simulation tools like **NS2**, **MetLab**, etc. are also available. The version of the tool used for the research work will be the latest version as per availability.

8. Place of Work and Facilities Available

The research work will be undertaken in the Laboratories available in the university campus and the software's and hardware's provided will be used as a part of the research work.

9. Limitations & Alternative Plan of the study

Some experiments and consultation may be required for the research work. Different labs may be used as per the requirement of the research.

10. References

[1] "Sensor Networks: Evolution, Opportunities and Challenges", Proceedings of the IEEE, Vol. 91. No. 8, August 2008.

[2] "A Survey on Wireless Sensor Networks Technology", Research Trends and Middleware's Role, University of Cambridge, 2005.

[3] "A Survey on Sensor Networks", IEEE Communication Magazine, August 2002.

[4] "System-Architecture for Sensor Networks Issues, Alternatives and Direction", ICCD'02, 2002.

[5] John A. Stankovic "Research Challenges for Wireless Sensor Networks", ACM SIGBED Review, 2004.

[6] Marcos Augusto M. Vieira, Diógenes Cecílio da Silva Junior, Claudionor N. Coelho. Jr., José M. da Mata "Survey on Wireless Sensor Network Devices", Emerging Technologies and Factory Automation, 2003. Proceedings. ETFA '03. IEEE Conference.

[7] A. Dunkels, T. Voigt, and J. Alonso. "Making TCP/IP Viable for Wireless Sensor Networks". In Proceedings of the First European Workshop on Wireless Sensor Networks (EWSN 2004), work-in-progress session, Berlin, Germany, Jan. 2004.

[8] Rodrigo Roman, Javier Lopez "Integrating Wireless Sensor Networks and the Internet: A Security Analysis", Internet Research, Volume 19 issue 2, Emerald, 2009.

[9] Z. Z. Marco, K. Bhaskar, "Integrating Future Large-scale Wireless Sensor Networks with the Internet", USC Computer Science Technical Report CS 03-792, 2003.

[10] Tanveer Zia, Albert Zomaya, "Security Issues in Wireless Sensor Networks", International Conference on Systems and Networks Communications, 2006. ICSNC '06, IEEE, 2006.

[11] C. Castelluccia, E. Mykletun, and G. Tsudik, (2005). "Efficient Aggregation of Encrypted Data in Wireless Sensor Networks," Proc. Second Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (Mobiquitous '05).

[12] Rachna. H and M.S. Patel, "Encryption and Key Management Approach with In-Network Processing in Wireless Sensor Network and Security Analysis", World Journal of Science and Technology 2011, 1(12): 46-49, ISSN: 2231 – 2587.

[13] Sadaqat Ur Rehman, Muhammad Bilal, Basharat Ahmad, Khawaja Muhammad Yahya, Anees Ullah, Obaid Ur Rehman, "Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN)", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012.

11. Appendix

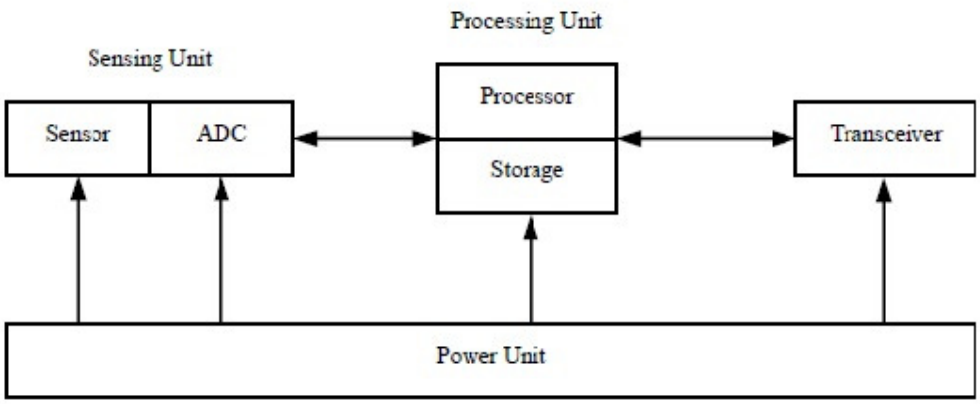


Fig. 1 Sensor Device Components

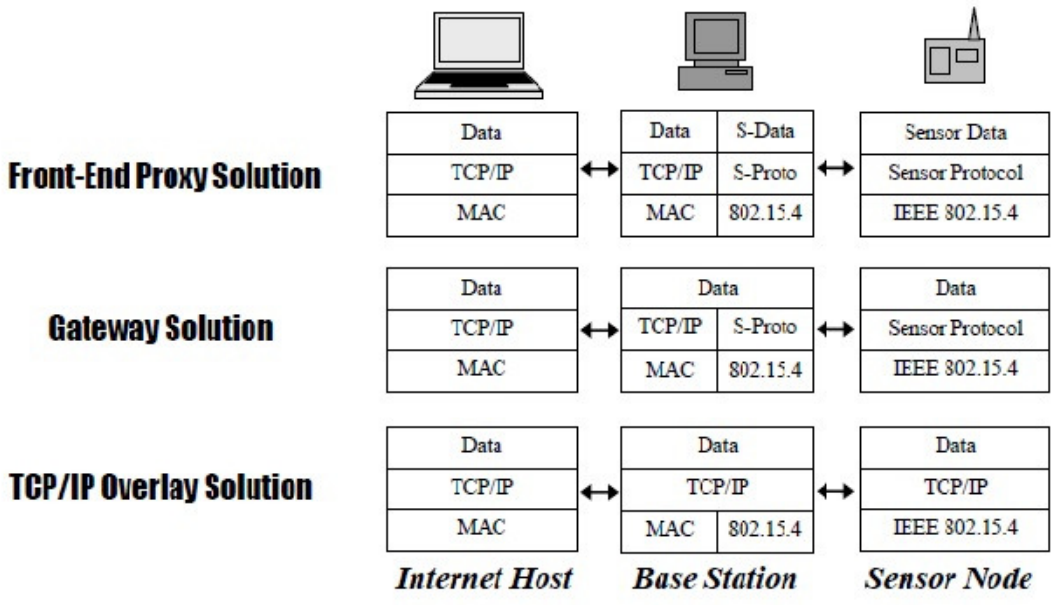


Fig. 2 Integration Strategies

	Traditional IP-Based Networks	Wireless Sensor Networks
Networking Mode	Application-independent	Application-specific
Routing Paradigms	Address-centric	Data-centric, Location-centric
Typical Data Flow	Arbitrary, One to one	To/from querying sink, One-to-many and many-to-one
Data Rates	High (Mbps)	Low (kbps)
Resource constraints	Bandwidth	Energy (battery-operated nodes), Limited processing and memory
Network Lifetime	Long (years-decades)	Short (days-months)
Operation	Attended, administered	Unattended, Self-configuring

Table 1: Key differences between traditional IP-based networks and wireless sensor networks